
[\[Date Prev\]](#)[\[Date Next\]](#)[\[Thread Prev\]](#)[\[Thread Next\]](#)[\[Date Index\]](#)[\[Thread Index\]](#)

Fw: IPSec vs. SSL

- *To:* <ipsec@lists.tislabs.com>
 - *Subject:* Fw: IPSec vs. SSL
 - *From:* "Venkat RK Reddy" <vpothams@cisco.com>
 - *Date:* Mon, 18 Dec 2000 16:19:56 -0800
 - *Sender:* owner-ipsec@lists.tislabs.com
-

IPSec's advantage over SSL: It has more flexibility on choosing the authentication mechanisms (like the PreSharedKey), and therefore makes it difficult for the attacker to do man in the middle. SSL is based only on public key and with tools (like dsniff2.3), its possible to do man in the middle breaking SSL.

SSL's advantage over IPSec: In SSL, the client and the server exchange * hash * over the "initial handshake" and therefore is difficult for an attacker to control (change the proposals that the client has sent so that the server chooses the proposals that attacker sends or whatever) the main mode "initial" handshake.

More discussion on this would be enlightening and appreciated.

- ---- Original Message -----

From: [Tim Lee](#)

To: ipsec@lists.tislabs.com

Sent: Saturday, December 16, 2000 5:30 PM

Subject: Re: IPSec vs. SSL

Are there any situations where it is useful to have IPSec in addition to SSL?

Follow-Ups:

- **Re: Fw: IPSec vs. SSL**
 - *From:* Rick Smith at Secure Computing <rick_smith@securecomputing.com>
-

- Prev by Date: **Re: IPSec vs. SSL**
- Next by Date: **Re: Fw: IPSec vs. SSL**
- Prev by thread: **Re: IPSec vs. SSL**
- Next by thread: **Re: Fw: IPSec vs. SSL**
- Index(es):
 - **Main**
 - **Thread**

S13	2267635	authentica\$5 approv\$5 verification verif\$5 secur\$4	US-PGPUB; USPAT; EPO; DERWENT	OR	OFF	2005/12/01 12:00
S14	4325930	user client person human member customer	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2005/12/01 12:01
S15	7726786	select\$5 elect\$4 chose\$4 choos\$4 choic\$4 pick\$3 designat\$4 indicat\$4	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2005/12/01 12:03
S16	5206300	menu\$3 window\$3 GUI (graphic\$4 adj2 user adj2 interfac\$3) interfac\$4 component\$4 display\$4	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2005/12/01 12:06
S17	125022	(S14 near3 S15) near10 S16	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2005/12/01 12:14
S18	8013	S17 same S13	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2005/12/01 12:08
S19	457	S18 and S12	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2005/12/01 12:08
S20	263	(@ad<"20010723" or @rlad<"20010723") and S19	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2005/12/01 12:50
S21	249	(@ad<"20010723" or @rlad<"20010723") and S19 and configur\$5	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2005/12/01 12:09
S22	116166	(S14 adj5 S15) near10 S16	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2005/12/01 12:17
S23	1234	S13 adj15 S22	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2005/12/01 12:49
S24	149	S23 and S12	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2005/12/01 12:49
S25	124	(@ad<"20010723" or @rlad<"20010723") and S24	US-PGPUB; USPAT; EPO; DERWENT	OR	ON	2005/12/01 12:50

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	2	"20030200321"	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	OFF	2005/12/02 09:31
S1	163	@ad<"20010723" and VPN and DHCP	US-PGPUB; USPAT; EPO; DERWENT	OR	OFF	2005/12/01 10:10
S2	12	@ad<"20010723" and VPN and (DHCP same allocate)	US-PGPUB; USPAT; EPO; DERWENT	OR	OFF	2004/10/13 11:51
S3	3	@ad<"20010723" and VPN and (DHCP same allocate) and (login same (webpage or server))	US-PGPUB; USPAT; EPO; DERWENT	OR	OFF	2004/10/13 17:58
S4	7	VPN and (DHCP same allocate) and (login same server)	US-PGPUB; USPAT; EPO; DERWENT	OR	OFF	2004/10/13 17:58
S5	40	"0039666"	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	OFF	2005/09/16 08:43
S6	1	"0039666".pn.	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	OFF	2005/09/16 08:42
S7	2183352	wo "0039666"	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	OFF	2005/09/16 08:43
S8	0	wo near2 "0039666"	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	OFF	2005/09/16 08:43
S9	4	kenneth near2 carlino	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	OFF	2005/09/16 13:43
S10	2	"6654607".pn.	US-PGPUB; USPAT; EPO; DERWENT; IBM_TDB	OR	OFF	2005/09/16 13:44
S11	32	("6061789" "6012088" "6067568" "6101543" "6119234" "6055236" "6196705" "5420926" "5884270" "6092198" "6076078" "6055518" "5961593" "5812670" "5636139" "6023510").pn.	US-PGPUB; USPAT; EPO; DERWENT	OR	OFF	2005/12/01 11:14
S12	10587	vpn "virtual private network"	US-PGPUB; USPAT; EPO; DERWENT	OR	OFF	2005/12/01 11:58